Reducing fraud in the information age

Technological advances, volatile markets and a continuing economic crisis make for fertile soil for fraud. Whether driven by need or greed, fraudsters keep the world's financial institutions under constant pressure. It is no longer enough just to investigate fraud after it happens, companies need to work individually and together to address the underlying roots of fraud and prevent it before it happens

What kind of fraud has become more common or more dangerous as a result of technological advances?

Vishal Marria, Detica NetReveal: Attacks against corporate accounts have become more common as financial institutions have rolled out web-based cash/treasury management solutions to their business customers. The availability of Trojan toolkits has increased the pool of potential fraudsters who can now readily procure the technology and know-how to commit online fraud. These attacks have become more dangerous because criminals are systematically probing financial institutions to discover weaknesses, which are then exploited for significant gain.

Daniel Barton, Alvarez & Marsal: Technology has made many types of fraud easier to conduct and harder to detect. The rise in the use of mobile devices means that not all emails sit on servers long enough to be recorded. For instance, an email sent by Blackberry and immediately deleted will not be on the server during back-up time – usually overnight. The sheer volume of data and the number of transactions makes detection harder, though this can be combatted through smart analysis using a range of forensic technology tools and techniques.

We also have a wider range of electronic data sources including Facebook, Twitter, instant messaging, Blackberry messaging and other social media platforms. Fraudsters are now better connected and more private information is publicly available. And, of course, most companies now have WiFi and other remote connection protocols, which create additional security vulnerabilities. But the technology to fight fraud has certainly improved, with detection and investigation tools becoming increasingly advanced and efficient – we are able to sift through larger and more complex data sets faster than ever before.

The Panel

Daniel Barton, Senior director, Alvarez & Marsal
Dean Goodlett, Assistant vice-president and fraud investigations manager in the financial intelligence unit, Rabobank
Vishal Marria, Director, Financial Services Solutions, Detica NetReveal

Dean Goodlett, Rabobank: What is not so clear is exactly what is meant by 'online banking account intrusion'. For instance, when an account takeover occurs, was the enabling factor an actual security breach within the financial institution, a viral invasion of the customer computer system, a fraudulent act by an authorised user of the account, or the result of the negligent use of social media? While the en- result may be the same, each method of entry into the account requires its own solution. I suggest dividing crimes into four categories: internal system intrusion, external system intrusion, abuse of privilege and negligence.

It is important to understand which poses the greatest threat. At present, although external system intrusions are gaining the greatest notoriety, the negligent release of information is driving the greatest number of online banking account intrusions. The number-one cause of account takeovers for 2010 was a change of address, followed by an added signer on the account. In each of these, there is no need for a system intrusion. Searching across social media or dumpster diving can provide all the information needed to telephone that helpful call centre and get the account information changed.

Vishal Marria, Director, Financial Services Solutions, Detica NetReveal

Vishal Marria joined Detica in 2005 and was instrumental in developing the NetReveal financial services solution. He has been deeply involved in creating financial risk strategies and developing solutions to counter a wide range of financial risk including insider fraud, first party fraud, application fraud, rogue trading, counterparty risk, credit risk and compliance. Vishal heads the Detica NetReveal global financial services team and is currently engaged with major banking and insurance companies around the world. He also has extensive experience in financial crime solutions for government and national security.

We are a global society that stores its banking information on the same unprotected system from which we send out our tweets. Perhaps the 'information age' could also be defined as that time in which we divulged too much information.

I cannot conclude without a brief look into what is often considered taboo. We can protect our own systems, we can educate our customers, we can monitor transactions – but how do we prevent attacks from within? This past year has been one of numerous arrests for 'account surfing'. We talk about preventing the negligent release of account information, but what about the merchandising of that information to the highest bidder?

How can firms co-operate more effectively on fraud prevention?

Vishal Marria: Ad-hoc information sharing is no longer sufficient to fight sophisticated and organised fraud, especially where fraud attacks can be sudden and high-impact. Institutions are beginning to acknowledge that the systematic sharing of intelligence can improve the bottom line for all member banks. While this represents data compliance and competitive challenges, the rewards can be significant.

Dean Goodlett: The problem here is twofold. First, while we all talk individually about co-operation, the fact is our organisations are competitors in the marketplace. And second, we are a litigation-prone global society.

Neither of the above is bad in itself – competition keeps us moving forward and litigation keeps us from solving our problems with violence. However, competition can prevent us from desiring success for those with whom we compete, and litigation can prevent us from sharing proprietary information.

Until we can overcome the problems inherent in both of the above, our efforts at co-operation will be limited to individual case assistance. The exceptions I find to this occur in seminar and conference settings. The actual instruction and panel discussions are invaluable for sharing solutions, and the personal networks established are often a very good manner in which to address a problem without committing the organisation to the issue.

At present, I believe seminars and conferences and the attendant networking are the most viable methods of disseminating information without invoking the restrictions imposed by competition and litigation. In the future, I would like to think we will move to implement a 'clearing-house' concept among organisations, in which questions could be asked and anonymity retained, both by those asking and those answering.

Daniel Barton: It is challenging for this to happen effectively in practice. Companies generally want to keep these kinds of issues internal to maintain a positive image for customers and competitors. In relation to bribery and corruption, we have seen some success with companies operating in the same industry in high-risk geographies collectively agreeing not to pay certain types of bribes or facilitation payments. This works if everybody sticks to the agreement, as a level playing field is maintained. Increased anti-bribery action across the world should increase the number of these agreements in the future.

What are the key points to remember if you are conducting the internal investigation of a fraud?

Daniel Barton: There are three points to remember: control and confidentiality, completeness and objectivity.

Knowledge of the investigation, certainly during the early stages, needs to be kept to a small number of key people. That way, control of the investigation is maintained and work can be conducted to substantiate the allegation without tipping off those that may have been involved. At the outset, you rarely know with certainty who may have been involved or how widespread the problem may be. Working out who can be trusted to assist with information gathering is a risk that can be managed by keeping the group small, senior and ideally two steps away from those that may be involved.

Ensuring you are obtaining all the potentially relevant data is also key. These days most people have a laptop computer, but you need to ask whether the person or people involved also have an old desktop computer that is still in use? It is essential to get the data from the hard drives of both computers. When interrogating financial systems, ensuring that all potentially relevant fields of information are being downloaded prevents either missing information or the need to go back and re-perform the task.

If suppliers are involved, it is important to have all applicable codes and references. There is often more than one code, especially where there are subsidiary companies or the supplier is doing business with the company in different countries.

Sometimes an allegation of fraud cannot be substantiated and, from time to time, has been made with purely malicious intent. Until you can prove what has occurred, the individuals involved should be treated objectively in case nothing is found. But you must always remain vigilant for any other type of fraud or non-compliance. When you commence an investigation you never know where the trail might lead you or what you might find out.

Vishal Marria: React quickly, be thorough and ensure you have a full audit trail. An internal member of staff could have high levels of access within the organisation, which could pose serious harm. Do not assume the individual is working alone. Equally, ensure the facts are correct and an intervention plan on a suspected fraud is clearly defined. This plan should allow for regular checkpoints with senior representation that can verify the findings once the suspected staff member is aware of the investigation – a false positive in the findings can have irreversible connotations.

Dean Goodlett: The most valuable lesson I have learned from internal investigations is that they are internal. What I mean is the nature of the internal investigation does not just involve interaction with internal situations, personnel and systems. There is also the internal motive side, and that must be considered when dealing with every person surrounding the investigation. The sad fact is that many internal investigations involve employees in addition to those named in the complaint. And, often those unnamed employees will present themselves as the most desirous of 'getting to the bottom of this'. The true goal of their offers of assistance is preventing knowledge of their own involvement or of protecting an associate. By keeping tabs on where you are going with the investigation, they can actually steer your efforts, and thereby manage the risk to themselves or others. Yes, it is risk management and, as such, these additional employees will have already invested heavily in plausible deniability protection.

Everyone involved in an internal investigation will have an internal agenda for why and how they react to the investigation. Do you know what the internal agenda is for each of these people? Then why would you consider revealing information to them?

What sort of personnel policies do firms need to have in place to reduce the risk of fraud?

Daniel Barton: Companies should undertake effective due diligence and background screening before hiring senior management and key functional employees. This should also be repeated and refreshed on a regular basis. Having everyone sign up to a clear, concise code of conduct and confirming annually that they have read, understood and comply with the policy is also helpful. Standard practices that have been around for a long time, but are not always properly enforced, include rotation of duties and mandatory holiday to be taken each year. However, policies can only get a company so far. Tone at the top and, importantly, tone at the middle are essential for breathing life into policies and turning them into part of the fabric of the business.

Daniel Barton, Senior director, Alvarez & Marsal

Dan Barton is a senior director with Alvarez & Marsal Global Forensic and Dispute Services in Europe. He specialises in fraud, bribery, corruption and regulatory issues, and has conducted investigations in several countries. Before joining Alvarez & Marsal, Dan was managing director in the Tokyo forensic services practice of PricewaterhouseCoopers.

Vishal Marria: Performing background checks and screening before an employee is granted full information access is essential, even for junior positions that traditionally may have been seen as low-risk. Ongoing monitoring of employees, associates and even suppliers against internal and external watch lists to flag possible connections to known high-risk individuals, should be part of a 'business-as-usual' policy. Many institutions are taking this a step further by analysing the risk associated with the social network of which the potential employee is a part. This significantly reduces the risk of bringing on board a member of staff who is colluding with fraudsters outside of the financial institution.

Dean Goodlett: For the most part, organisations are very good at knowing their new hires. Unfortunately, we do not commit to an ongoing programme of knowing our employees. Once they are hired, we move on. But sadly, situations change for our personnel, and all too often fraud is the manifested result.

Ideally, we would continue to monitor our employees for what is occurring in their lives. But, of course, there is the privacy issue and we can all be grateful it is in place. Besides, even if we knew our employees were facing tough times, what would we do? Would we watch them closely, keep them from being placed in tempting situations, spread our processes among multiple individuals, or implement checks and balances to prevent fraud?

Wouldn't it be smarter to just put those practices into place at first? Wouldn't it be wiser to attack our processes and procedures rather than our people?

Obviously, we do need personnel standards. And those standards should reflect a no-tolerance stance towards fraud from the top down. They should clearly delineate those areas in which the employee has no expectation of privacy. They should advise the employee to report suspicious activity. A copy should be reviewed and signed by the employee. But, even with all this in place, shouldn't we also make every effort to fraud-proof our job descriptions?

People change – the best policies are those that recognise this and place due diligence on the processes and procedures conducted by those people.

Frauds are running for longer and getting larger before detection. Why is this? And what can be done about it?

Vishal Marria: Fraudsters are running sophisticated and complex businesses, and they spend considerable time and effort testing organisations' systems to allow their activities to remain undetected. A typical large fraud may attack an organisation from multiple angles through different lines of business, channels or products. If organisations are not able to leverage their data effectively to realise a single view of the customer across the enterprise, they can miss the bigger picture and are often unable to detect the organised fraud until too late. Organisations must work proactively to leverage their data to protect their businesses – being preventative, not just reactive.

Daniel Barton: Conducting regular fraud risk analysis is a good way of ensuring that your controls are being tested and that gaps are spotted, so that fraud can be prevented – or at least made more difficult to commit. Companies should encourage employees to speak up if they become aware of anything that makes them uncomfortable. The employee does not have to make an accusation that fraud has actually taken place – this is the role of departments such as legal or compliance – but they should be encouraged to speak up and should be provided with an easy means of doing so. These means would include confidential telephone lines and email addresses, visible and active compliance representatives, and an open-door policy for all management.

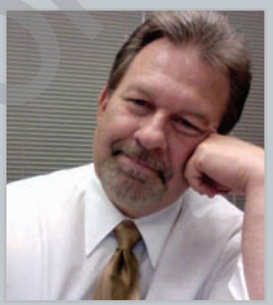
Dean Goodlett: Fraud is an ever-evolving issue that has embraced technology for new implementations and for the ability to change its forms. This has enabled fraud to adapt in order to attack new weak points, and to hide until new detection methods are developed. It has also greatly shortened the amount of time necessary to complete the fraud, as transactions are now completed at the speed of the internet. Therefore a new fraud scheme – or, more often, a repackaged old scheme – can involve a great number of internet-speed transactions before a problem is realised. Add to this the fact the return-on-investment issue prevents most organisations from investing in a solution for a problem they do not yet have or do not think they have. And when the economy is down, what is the first department to be cut?

The point here is that the fraudsters are better prepared, better hidden, have much less exposure time during the enactment, and are very difficult to discover when the decision has been made to not look.

But the greatest problem we face is the attitude of 'set it, forget it'. We put the safeguards in place and then go back to business. Unfortunately for the fraudsters, the pursuit of business endeavours involves looking for new weaknesses. Ongoing vigilance is a must and the effort must be a concerted one. Software updates, staff training, activity monitoring, customer education and constant vigilance must all be in place or else a weak point will be discovered by those who are looking to find it.

We talk much about combining forces globally to attack the fraud issue. I am all for that. But there are better ways to manage the fraud even within our own organisations. There needs to be a concerted buy-in from the entire organisation to cumulatively attack the fraud picture. I am referring to the Financial Intelligence Unit concept, in which all aspects of the fraud picture are combined under one roof. This involves a shared database and communication between all of those offices that are involved in investigations and monitoring, giving a multi-level and cross-channel view of fraud. Something I am looking at today may have been researched in an anti-money laundering investigation three years ago. Without their input, I am duplicating the efforts and may even miss a lead that is sitting dormant in their database. Only by making use of all the available intelligence can we move forward not only in our response to fraud, but also in preventive efforts as we seek to be truly cross-channel and allow for real-time decision-making.

Dean Goodlett, Assistant vice-president and fraud investigations manager in the financial intelligence unit, Rabobank



Dean Goodlett is the fraud investigations manager for the California division of Rabobank. He received his formal fraud training during a 24-year career in Los Angeles area law enforcement investigations, and holds professional certifications from both the Association of Certified Fraud Examiners and the Association of Certified Anti-Money Laundering Specialists.